

Ogłoszenie

Numer

2026-109067-262594

Id

262594

Powstaje w kontekście projektu

KPOD.05.10-IW.06-0001/25 - Przeprowadzenie szkoleń w formie e-learningowej z cyberbezpieczeństwa i systemu zarządzania bezpieczeństwem informacji dla pracowników oraz kadry kierowniczej w ramach Projektu Cyberbezpieczny Rząd

Tytuł

Przeprowadzenie szkoleń w formie e-learningowej z cyberbezpieczeństwa i systemu zarządzania bezpieczeństwem informacji dla pracowników oraz kadry kierowniczej Ministerstwa Energii w ramach Projektu Cyberbezpieczny Rząd.

Załączniki

Dodane do ogłoszenia w obowiązującej wersji z dn. 2026-01-29

1. Zapytanie ofertowe
2. Formularz oferty wraz z załącznikami

Czy dopuszczalna oferta częściowa?

NIE

Data opublikowania ogłoszenia

2026-01-29

Data ostatniej zmiany

2026-01-29

Termin składania ofert

2026-02-06 10:00:00

Planowany termin podpisania umowy

2026-02

Dane adresowe ogłoszeniodawcy

Ministerstwo Energii
Przemysłowa 26
00-450 Warszawa
NIP: 9542867467

Osoby do kontaktu

Ewa Biolik
tel.: +48 32 433 42 01
e-mail: ewa.biolik@me.gov.pl

Kinga Skibińska
tel.: +48 32 433 42 07
e-mail: kinga.skibinska@me.gov.pl

Części zamówienia

Część: 1

Tytuł części 1

Przeprowadzenie szkoleń w formie e-learningowej

Czy dopuszczalne oferty wariantowe

NIE

Przedmioty zamówienia do części 1

Typ

Usługa

Podkategoria

Usługi szkoleniowe

Opis

Przedmiotem umowy jest przeprowadzenie szkoleń w formie e-learningowej z cyberbezpieczeństwa i systemu zarządzania bezpieczeństwem informacji dla pracowników oraz kadry kierowniczej Ministerstwa Energii.

I. Temat szkolenia - część I: Podstawy cyberbezpieczeństwa i cyberhigieny.

II. Cel szkolenia - część I: Podniesienie poziomu świadomości pracowników Ministerstwa Energii w zakresie cyberbezpieczeństwa, zapobiegania incydom oraz wdrożenia nawyków cyberhigieny w codziennej pracy z systemami teleinformatycznymi zgodnie z wymaganiami ustawy o Krajowym Systemie Cyberbezpieczeństwa.

III. Zakres i program szkolenia – część I:

Moduł 1. Wprowadzenie do cyberbezpieczeństwa - zrozumienie podstawowych pojęć i kontekstu bezpieczeństwa informacji w administracji publicznej:

- definicje i podstawowe pojęcia (atak, podatność, incydent, zagrożenie, ryzyko),
- bezpieczeństwo informacji a ochrona danych osobowych (powiązanie z RODO),
- krajowy system cyberbezpieczeństwa i obowiązki instytucji publicznych,
- rola i odpowiedzialność pracownika w systemie bezpieczeństwa.

Moduł 2. Najczęstsze zagrożenia w środowisku pracy - identyfikacja i rozpoznawanie realnych zagrożeń.

- phishing, smishing, vishing – przykłady rzeczywistych kampanii wymierzonych w administrację,
- złośliwe oprogramowanie (ransomware, spyware, trojany, keyloggers),
- socjotechnika – jak działa manipulacja i jak jej unikać,
- fake news i dezinformacja – rozpoznawanie i reagowanie,
- zagrożenia wewnętrzne (nieumyślne działania pracowników, błędna konfiguracja).

Moduł 3. Cyberhigiena i dobre praktyki - codzienne nawyki bezpieczeństwa.

- polityka haseł: tworzenie silnych haseł, menedżery haseł, MFA,
- zasady korzystania z poczty elektronicznej i komunikatorów (załączniki, linki, weryfikacja nadawcy),
- bezpieczne przeglądanie Internetu i korzystanie z zasobów sieciowych,
- ochrona urządzeń mobilnych (PIN, szyfrowanie, aktualizacje),
- praca zdalna i zdalny dostęp do systemów Ministerstwa – VPN, szyfrowanie danych,
- czyszczenie biurka i ekranu (zasada „czystego biurka” i „czystego ekranu”),
- bezpieczeństwo fizyczne i ochrona nośników danych (USB, dokumenty papierowe).

Moduł 4. Reagowanie na incydenty - umiejętność właściwego zachowania w sytuacji zagrożenia.

- jak rozpoznać symptomy incydentu (nietypowe działanie systemu, komunikaty, żądania danych),
- co zrobić w przypadku podejrzenia ataku lub błędu użytkownika,

- procedura zgłaszania incydentów w Ministerstwie (kanały, osoby kontaktowe, eskalacja),
- przykłady skutecznego reagowania (case studies).

Moduł 5. Odpowiedzialność prawna i etyczna -uświadomienie konsekwencji prawnych i organizacyjnych.

- obowiązki pracowników w zakresie ochrony danych osobowych,
- konsekwencje naruszenia zasad bezpieczeństwa (dyscyplinarne, finansowe, reputacyjne),
- etyka cyfrowa – odpowiedzialne korzystanie z zasobów IT, prywatność w sieci.

Moduł 6. Testy i ćwiczenia praktyczne - utrwalenie wiedzy i ocena skuteczności szkolenia.

- analiza przykładowych e-maili phishingowych,
- symulacja procedury zgłoszenia incydentu,
- omówienie błędów i najlepszych praktyk.

Moduł 7. Podsumowanie i rekomendacje

- najważniejsze zasady cyberhigieny („10 złotych zasad bezpieczeństwa”),
- wskazówki dotyczące dalszego samokształcenia,
- informacje o kanałach wsparcia.

IV.☒ Temat szkolenia – część II: Wymagania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym ochrona danych osobowych.

V.☒ Cel szkolenia - część II: Zapoznanie wszystkich pracowników Ministerstwa Energii z wymaganiami SZBI.

VI.☒ Zakres i program szkolenia – część II:

Moduł 1. Podstawy normy ISO/IEC 27001 i SZBI w administracji publicznej:

- Polityka Bezpieczeństwa Informacji – cele, zakres, zasady stosowania,
- Procedury i instrukcje SZBI – zarządzanie dostępem, praca zdalna, kopie zapasowe, reagowanie na incydenty,
- Instrukcje operacyjne (np. obsługa nośników danych, korzystanie z poczty, polityka haseł),
- Klasyfikacja informacji – kategorie poufności, oznaczanie dokumentów,
- Zasady ochrony informacji niejawnych i służbowych,
- powiązanie między dokumentacją SZBI a polityką bezpieczeństwa IT oraz zarządzeniami wewnętrznymi kierownictwa.

a.☒ Wykonawca w terminie do 5 dni od daty podpisania umowy, przedłoży do akceptacji projekt programu szkolenia (scenariusz/storyboard).

b.☒ Zamawiający ma prawo zgłosić uwagi do treści w terminie 3 dni roboczych. Wykonawca zobowiązany jest do naniesienia poprawek w ramach wynagrodzenia.

c.☒ W terminie 2 dni od akceptacji projektu, Zamawiający prześle Wykonawcy, za pośrednictwem poczty elektronicznej imienną listę Uczestników Szkolenia wraz z adresami e-mail.

d. W terminie 2 dni od dnia przekazania danych Uczestników, Wykonawca przekaże Uczestnikom Szkolenia, na ich adresy e-mail, hasła z danymi dostępowymi do Szkolenia, umożliwiającymi korzystanie z niego.

e. Uruchomienie szkolenia dla pracowników może nastąpić wyłącznie po uzyskaniu akceptacji ostatecznej wersji treści przez Zamawiającego.

f. Wykonawca zobowiązuje się do zachowania poufności otrzymanych materiałów i wykorzystania ich wyłącznie w celu realizacji zamówienia. Wykonawca podpisze stosowne zobowiązanie do powierzenia przetwarzania danych osobowych.

VII. Grupa szkoleniowa: wszyscy pracownicy Ministerstwa Energii.

VIII. Liczba uczestników i forma szkolenia: Licencja na maksymalnie 350 dostępów, na platformie e-learningowej Wykonawcy, w trybie on-line (24 godziny na dobę / 7 dni w tygodniu).

a. Dostępny dla 350 pracowników będą aktywne przez okres dwóch miesięcy od dnia uruchomienia szkolenia.

b. Szkolenie (Część I i Część II łącznie) musi obejmować materiał dydaktyczny przewidziany na minimum 3 godziny lekcyjne (3 x 45 minut) przeciętnego czasu pracy użytkownika z materiałem.

IX. Wymagania techniczne i jakościowe platformy

a. Platforma e-learningowa musi być dostępna w modelu SaaS (Software as a Service) przez standardowe przeglądarki internetowe (min. Chrome, Firefox, Edge, Safari) bez konieczności instalowania dodatkowego oprogramowania przez użytkownika.

b. Platforma musi być w pełni responsywna (RWD) – umożliwiać poprawne wyświetlanie i realizację szkolenia na urządzeniach mobilnych (smartfon, tablet).

c. Wykonawca gwarantuje dostępność platformy na poziomie min. 99% w skali miesiąca.

d. Wykonawca zapewni wsparcie techniczne (Helpdesk) dla użytkowników w dni robocze w godzinach 8:00–16:00, z czasem reakcji na zgłoszenie błędu nie dłuższym niż 24h.

e. Przedmiot zamówienia (zarówno platforma e-learningowa, jak i sama treść szkolenia) musi być w pełni zgodny z wymaganiami określonymi w załączniku do Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, tj. odpowiadać standardowi WCAG 2.1 na poziomie AA, w tym:

i. Napisy: Wszystkie materiały audio i wideo muszą posiadać napisy dla osób niesłyszących i niedosłyszących, zsynchronizowane z dźwiękiem.

ii. Alternatywa tekstowa: Wszystkie elementy nietekstowe (grafiki, schematy, ikony) istotne dla przekazu muszą posiadać opisy alternatywne (atrybut alt).

iii. Kontrast: Stosunek kontrastu tekstu do tła musi wynosić co najmniej 4.5:1 (zgodnie z wytycznymi WCAG).

iv. Nawigacja klawiaturą: Wszystkie elementy interaktywne szkolenia (przyciski, nawigacja, zadania testowe) muszą być w pełni obsługiwane za pomocą samej klawiatury (bez użycia myszki).

- v.☒ Czytniki ekranu: Kod szkolenia i platformy musi być poprawnie interpretowany przez programy czytające dla osób niewidomych (np. NVDA, JAWS).
- f.☒ Wykonawca wraz z udostępnieniem szkolenia przekaże Zamawiającemu wypełnioną listę sprawdzającą (raport z audytu dostępności) potwierdzającą spełnienie wytycznych WCAG 2.1 AA lub aktualną Deklarację Dostępności dla platformy.
- g.☒ Wykonawca zobowiązany jest do pełnego oznakowania platformy e-learningowej oraz wszelkich materiałów szkoleniowych zgodnie z zasadami promocji projektów finansowanych z Krajowego Planu Odbudowy (KPO), w szczególności zgodnie z aktualną „Księgą Identyfikacji Wizualnej KPO”
- h.☒ Oznakowanie, o którym mowa w ust. g, obejmuje w szczególności:
 - i.☒ umieszczenie wymaganych logotypów (m.in. barwy narodowe, logo KPO, logo UE – NextGenerationEU) w widocznym miejscu (np. nagłówek strony);
 - ii.☒ umieszczenie logotypów oraz informacji o współfinansowaniu na slajdach, w materiałach wideo (np. ekran początkowy i końcowy) oraz w dokumentach dodatkowych;
 - iii.☒ umieszczenie pełnego zestawu wymaganych znaków graficznych oraz informacji o projekcie „Cyberbezpieczny Rząd” na imiennych zaświadczeniach o ukończeniu szkolenia;
 - iv.☒ zamieszczenie na początku szkolenia planszy informującej o celu szkolenia i źródle jego finansowania.
- i.☒ Zamawiający przekaże Wykonawcy niezbędne logotypy oraz wytyczne w terminie 2 dni od podpisania umowy. Wykonawca ponosi pełną odpowiedzialność za prawidłowość naniesienia znaków graficznych zgodnie z otrzymaną instrukcją.
- X.☒ Zaświadczenie potwierdzające odbycie szkolenia: Szkolenie dla każdego użytkownika musi zakończyć się możliwością wygenerowania zaświadczenia potwierdzającego odbycie szkolenia w formie on-line na platformie Wykonawcy.
 - a.☒ Platforma musi automatycznie wygenerować imienne zaświadczenie potwierdzające odbycie szkolenia w formacie PDF.
 - b.☒ Zaświadczenie musi zawierać: imię i nazwisko pracownika, datę ukończenia, nazwę szkolenia oraz logotypy Zamawiającego
 - c.☒ Pracownik musi mieć możliwość samodzielnego pobrania zaświadczenia w dowolnym momencie trwania licencji.
 - d.☒ Wykonawca zapewni wskazanym pracownikom Zamawiającego dostęp do panelu administratora lub będzie przysyłał cykliczne raporty z postępów szkolenia.
 - e.☒ W terminie do 2 dni roboczych od dnia zakończenia okresu udostępnienia szkolenia (lub od dnia, w którym wszyscy Uczestnicy ukończyli szkolenie), Wykonawca przekaże Zamawiającemu drogą elektroniczną na adres: sekretariatdcb@me.gov.pl kompletną dokumentację potwierdzającą realizację przedmiotu w tym komplet kopii zaświadczeń wszystkich Uczestników, w formacie plików PDF.
 - f.☒ Raport musi zawierać co najmniej:
 - i.☒ listę osób uprawnionych

Kody CPV

80510000-2 Usługi szkolenia specjalistycznego

Miejsca realizacji

cała Polska

Kraj

Polska

Warunki, jakie musi spełniać oferent

Typ

Dodatkowe warunki udziału

Opis

4. W celu potwierdzenia braku podstaw do wykluczenia wykonawca zobowiązany jest złożyć wraz z ofertą oświadczenia, zgodne ze wzorami oświadczeń, stanowiącymi załączniki nr 4 i 5 do Zaproszenia tj. OŚWIADCZENIE WYKONAWCY

O BRAKU PODSTAW DO WYKLUCZENIA Z POSTĘPOWANIA

oraz OŚWIADCZENIE WYKONAWCY O BRAKU KONFLIKTU INTERESÓW (Przez powiązania kapitałowe lub osobowe rozumiem wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przeprowadzeniem procedury wyboru Wykonawcy, a Wykonawcą, polegające w szczególności na:

- 1) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
- 2) posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa,
- 3) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
- 4) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.
- 5) pozostawaniu z Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przeprowadzeniem procedury wyboru Wykonawcy, a Wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia).

Kryteria oceny do części 1

Czy kryterium cenowe?

TAK

Opis

1. Przy wyborze najkorzystniejszej oferty spośród ofert niepodlegających odrzuceniu Zamawiający będzie stosował kryterium ceny.

2. Przyjęto liczbę 100 jako maksymalną liczbę punktów, którą może uzyskać każdy z Wykonawców, według poniższych kryteriów przy czym 1% = 1 pkt.

cena - 100% (100pkt)

Podsumowanie

Oś czasu związana z ogłoszeniem i ofertowaniem

-> 2026-01-29 - data opublikowania



-> 2026-02-06 10:00:00 - termin składania ofert



-> 2026-02 - planowany termin podpisania umowy

Oś czasu realizacji przedmiotów zamówienia

Brak zdefiniowanych etapów dla przedmiotów zamówienia.